Airband Communications, Inc.

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for calendar year 2007.

Name of company covered by this certification: Airband Communications, Inc.

Form 499 Filer ID: 825978

Name of signatory: Lynn McNeill

Title of signatory: Officer

I, Lynn McNeill, certify that I am an officer of the company named above ("Company"), and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Federal Communications Commission's ("Commission") Customer Proprietary Network Information ("CPNI") rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI. The Company has not taken any actions (proceedings instituted or petitions filed at either state commissions, in the judicial system, or at the Commission) against data brokers during the past year. The Company also has no knowledge or experience regarding the specific processes pretexters are using to attempt to access CPNI. The steps that the Company is taking to protect CPNI are described in the attached statement that summarizes the Company's operating procedures for compliance with the Commission's CPNI rules.

This certification is made to the best of my knowledge, information and belief.

Signed: _____

Dated: 9/25/08

STATEMENT REGARDING OPERATING PROCEDURES
GOVERNING CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)

The following statement explains the operating procedures of Airband Communications, Inc. ("Company") to ensure compliance with the Customer Proprietary Network Information ("CPNI") rules of the Federal Communications Commission ("Commission" or "FCC").

1. To the extent the Company accesses or maintains CPNI, the Company uses, discloses and permits access to CPNI only for the purpose of (a) providing a customer with the requested service; (b) to initiate, render, bill, and collect for its telecommunications services; (c) to provide inbound telemarketing, referral, or administrative services to subscribers for the duration of the call, if such call is initiated by the subscriber and the subscriber approves of the use of such CPNI to provide such service; or (d) for the purpose of providing customer premises equipment ("CPE").

2. The Company does not use, disclose or permit access to CPNI for outbound marketing purposes (either internally or by third parties).

3. The Company does not provide Call Detail Record ("CDR") information over the telephone to customers who contact the Company. The Company also does not provide access to any CPNI (CDR or non-CDR) on-line. The Company does not have any retail locations.

4. The Company will disclose CPNI upon affirmative written request or telephone request by a customer, but does not provide such CPNI over the telephone, but instead by sending it to the customer's address of record.

5. Within 7 days of a reasonable determination of breach (*i.e.*, CPNI disclosed to a third party without customer authorization), the Company will notify the US Secret Service ("USSS") and Federal Bureau of Investigation ("FBI") of the breach via the central reporting facility www.fcc.gov/eb/cpni.

    - After 7 days of USSS and FBI notice, if the Company has not received written direction from the USSS or FBI, the Company will notify the customer of the breach, unless the USSS and FBI have extended the period for such notice.

    - For 2 years following USSS and FBI notice, the Company will maintain a record of (1) discovered breaches; (2) any notifications to the USSS and FBI; (3) any USSS and FBI responses; (4) the dates any breaches were discovered; (5) the dates INS notified USSS and FBI; (6) a detailed description of any CPNI that was breached; and (7) the circumstances of any such breaches.

6. The Company's employees are trained as to the proper protection, uses and treatment of CPNI, including familiarity with the Company's internal CPNI policies and procedures.

7. The Company employs a policy with appropriate remedies should any employee violate the Company's internal CPNI policies and procedures. Remedies may include, but are not limited to, financial, legal or disciplinary actions, including termination and referrals to law enforcement when appropriate.